

FILED

2017 OCT 13 PM 12:36

U.S. MAGISTRATE JUDGE

BY \_\_\_\_\_



SEALED

Office of the United States Attorney  
District of Nevada  
501 Las Vegas Boulevard, Suite 1100  
Las Vegas, Nevada 89101  
(702) 388-6336

FILED

2017 OCT 13 PM 12:36

U.S. MAGISTRATE JUDGE

BY \_\_\_\_\_

STEVEN W. MYHRE  
Acting United States Attorney  
District of Nevada  
CRISTINA D. SILVA  
PATRICK BURNS  
Assistant United States Attorneys  
501 Las Vegas Blvd. South, Ste. 1100  
Las Vegas, Nevada 89101  
Telephone: (702) 388-6336  
Fax (702) 388-6698  
[john.p.burns@usdoj.gov](mailto:john.p.burns@usdoj.gov)

Attorney for the United States of America

UNITED STATES DISTRICT COURT  
DISTRICT OF NEVADA

-oOo-

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
EMAIL ACCOUNT  
CENTRALPARK1@LIVE.COM THAT IS  
STORED AT A PREMISES  
CONTROLLED BY MICROSOFT.

A1

Magistrate No.

AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR SEARCH  
WARRANTS

(Under Seal)

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
EMAIL ACCOUNT  
MARILOUROSES@LIVE.COM THAT IS  
STORED AT A PREMISES  
CONTROLLED BY MICROSOFT.

A2

Magistrate No. 2:17-mj-01010-NJK

AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR SEARCH  
WARRANTS

(Under Seal)

STATE OF NEVADA     )  
                                  ) ss:  
COUNTY OF CLARK    )

///

///

**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION FOR SEARCH WARRANTS**

I, Zachary C. McKinney, Special Agent, Federal Bureau of Investigation (FBI),  
having been duly sworn, hereby depose and say:

**INTRODUCTION AND AGENT BACKGROUND**

1. Your Affiant makes this affidavit in support of an application for search warrants for information associated with email accounts centralpark1@live.com ("Target Account 1") and marilouroses@live.com ("Target Account 2"). Target Account 1 is an account associated with STEPHEN PADDOCK. Target Account 2 is an account associated with MARILOU DANLEY. The information associated with both accounts is stored at a premises owned, maintained, controlled, or operated by Microsoft Corporation ("Microsoft"), an American multinational technology company based in Redmond, Washington that specializes in Internet-related services and products along with the development and manufacturing of computer-related items. Those online services include, but are not limited to, email services, cloud computing, and many other services. The information to be searched is described in the following paragraphs and in Attachment "A" (attached hereto and incorporated herein by reference). This affidavit is made in support of an application for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Microsoft to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the Target Accounts.

2. I am a Special Agent with the Federal Bureau of Investigation, currently assigned to Las Vegas, Nevada. I have been employed as a Special Agent of the FBI since

1 March of 2017. Over the course of my employment with the FBI, I have conducted  
2 surveillance, analyzed telephone records, interviewed witnesses, supervised activities of  
3 sources, executed search warrants, and executed arrest warrants. These investigative  
4 activities have been conducted in conjunction with a variety of investigations, to include  
5 those involving robbery, drug trafficking, human trafficking, criminal enterprises, and  
6 more. In addition to my practical experiences, I received five months of extensive law  
7 enforcement training at the FBI Academy. Previous to the FBI, I was employed as a  
8 human intelligence gatherer with the United States Army. I was trained extensively in  
9 interrogation, interview, and source handling techniques and best practices. I also  
10 received an MBA in International Business and worked with ExxonMobil as a financial  
11 manager.

12 3. I make this affidavit in support of an application for a search warrant for  
13 information associated with the Microsoft accounts associated with  
14 centralpark1@live.com” and “marilouroses@live.com,” which is stored at a premises  
15 owned, maintained, controlled, or operated by Microsoft Corporation, headquartered at  
16 One Microsoft Way, Redmond, WA 98052-6399, hereinafter referred to as “premises,”  
17 and further described in Attachments A-1 and A-2 hereto.

- 18 a. Destruction/Damage of Aircraft or Aircraft Facilities - 18 U.S.C.A. § 32(a);  
19 b. Violence at International Airport - 18 U.S.C. § 37(a)(2); and  
20 c. Unlawful Interstate Transport/Delivery of Firearms by Non Federal  
21 Firearms Licensee – 18 U.S.C. §§ 922(a)(3) and (5);  
22 d. Aiding and Abetting – 18 U.S.C. § 2.

1 (hereafter, "Subject Offenses") have been committed by STEPHEN PADDOCK,  
2 MARILOU DANLEY, and others yet unknown. There is also probable cause to search  
3 the information described in Attachment "A" for evidence of these crimes and  
4 information which might reveal the identities of others involved in these crimes, as  
5 described in Attachment "B" (attached hereto and incorporated herein by reference).

6 **PROBABLE CAUSE**

7 4. On the evening of Sunday, October 1, 2017, Route 91 Harvest, a music  
8 festival, was in progress at 3901 South Las Vegas Boulevard, Las Vegas, Nevada. At  
9 approximately 10:08 p.m., the Las Vegas Metropolitan Police Department (LVMPD)  
10 received calls reporting shots had been fired at the concert and multiple victims were  
11 struck. LVMPD determined the shots were coming from Rooms 134 and 135 on the 32nd  
12 floor of the Mandalay Bay Resort and Casino, located due west of the festival rounds at  
13 3950 South Las Vegas Boulevard, Las Vegas, Nevada. These rooms are an elevated  
14 position which overlooks the concert venue. Witness statements and video  
15 footage captured during the attack indicates that the weapons being used were firing in  
16 a fully-automatic fashion.

17 5. LVMPD officers ultimately made entry into the room and located an  
18 individual later identified as Stephen Paddock. Paddock was deceased from an apparent  
19 self-inflicted gunshot wound.

20 6. Paddock's Nevada driver's license was located in the Mandalay Bay hotel  
21 room with Paddock, and both hotel rooms were registered in his name. A player's club  
22 card in name of Marilou Danley was located in Paddock's room, and the card returned  
23 to the address located on Babbling Brook Street in Mesquite, Nevada. FBI Agents  
24

1 located Danley, who was traveling outside the United States at the time of the  
2 shooting. It was ultimately determined that Danley resided with Paddock at the  
3 Babbling Brook address.

4 7. On October 2, 2017, search warrants were executed on Paddock's Mandalay  
5 Bay hotel rooms, Paddock's vehicle at Mandalay Bay, and two Nevada residences owed  
6 by Paddock: 1372 Babbling Brook Court in Mesquite, and 1735 Del Webb Parkway in  
7 Reno, Nevada. Officers and Agents found over 20 firearms, hundreds of rounds of  
8 ammunition, and hundreds of spent shell casings in the Mandalay Bay hotel rooms, in  
9 close proximity to Paddock's body. Over a thousand rounds of rifle ammunition and 100  
10 pounds of explosive material was found in Paddock's vehicle. Additional explosive  
11 material, approximately 18 firearms, and over 1,000 rounds of ammunition was located  
12 at the Mesquite residence. A large quantity of ammunition and multiple firearms were  
13 recovered from the Reno residence.

14 8. As of this date, 58 people have been identified to have been killed in  
15 Paddock's attack and another 557 were reportedly injured. Additionally, investigators  
16 discovered that STEPHEN PADDOCK also utilized a firearm to shoot large fuel tanks  
17 on Las Vegas McCarran International Airport property. Multiple bullet holes were found  
18 on the tank, which investigators believe was an attempt by STEPHEN PADDOCK to  
19 cause the tanks to explode.

20 9. In an effort to determine whether or not STEPHEN PADDOCK was  
21 assisted and/or conspired with unknown individuals, investigators have attempted to  
22 identify all of STEPHEN PADDOCK's associated. It was quickly determined that a  
23 casino player's card in the name of MARILOU DANLEY was located in the room at the  
24

1 time of the attack. She has been identified thus far as the most likely person who aided  
2 or abetted STEPHEN PADDOCK based on her informing law enforcement that her  
3 fingerprints would likely be found on the ammunition used during the attack.  
4 Subsequently, investigators worked to identify the communication facilities utilized by  
5 STEPHEN PADDOCK and MARILOU DANLEY.

6 10. Based on a review of STEPHEN PADDOCK's financial accounts, Target  
7 Account 1 was determined to belong to STEPHEN PADDOCK. On October 3, 2017,  
8 investigators requested an emergency disclosure of records from Microsoft related to  
9 Target Account 1 so it could be immediately searched for any evidence of additional co-  
10 conspirators. Unfortunately, the information was only requested for a six-month  
11 timeframe. Within the account, investigators identified Target Account 2 as one that  
12 belonged to MARILOU DANLEY, which was clear based on the communications  
13 between the two email accounts. In an interview, DANLEY stated that PADDOCK had  
14 access to one of her email accounts, which investigators believe to be Target Account 2.

15 11. On September 25, 2017, an email was exchanged between the Target  
16 Accounts which discussed a wire transfer of funds which was to be sent by STEPHEN  
17 PADDOCK to MARILOU DANLEY. It is unclear what the purpose of the wire transfer  
18 was, but MARILOU DANLEY is known to have been in the Philippines at the time.

19 12. Additionally, on July 6, 2017, Target Account 1 sent an email to  
20 centralpark4804@gmail.com which read, "try an ar before u buy. we have huge selection.  
21 located in the las vegas area." Later that day, an email was received back from  
22 centralpark4804@gmail.com to Target Account 1 that read, "we have a wide variety of  
23 optics and ammunition to try." And lastly, Target Account 1 later sent an email to  
24

1 centralpark4804@gmail.com that read, "for a thrill try out bumpfire ar's with a 100  
2 round magazine." Investigators believe these communications may have been related to  
3 the eventual attack that occurred at the Mandalay Bay in Las Vegas.

4 13. Your Affiant believes the requested search warrants will yield significant  
5 information from Microsoft such as STEPHEN PADDOCK's and MARILLOU DANLEY's  
6 contact lists, email messages content, IP address usage, photographs, third-party  
7 applications associated with the account, and more, which may constitute evidence of  
8 the planning of the attack and potentially identify other participants in the attack.  
9 Ultimately, your Affiant strongly believes the requested information will lead  
10 investigators to determine the full scope of STEPHEN PADDOCK's plan and MARILLOU  
11 DANLEY's possible involvement.

12 14. Investigators have previously sought and obtained a search warrant to  
13 examine the contents of both Target Accounts 1 and 2. After execution of that warrant,  
14 however, it became apparent and was confirmed with Microsoft that Microsoft was  
15 refusing to provide data related to/contained in the OneDrive online storage files for  
16 either account. Microsoft indicated to investigators that it did not believe such  
17 information was encompassed by the items to be produced that were specified in the  
18 original warrant. Investigators believe therefore that there is additional evidence  
19 Microsoft currently possesses that relates to the OneDrive online storage service, as well  
20 as potentially in a suite of other online services that Microsoft offers, including Office  
21 365, Windows Live Mail, Windows Live Writer, Windows Photo Gallery, Windows Live  
22 Messenger, Microsoft Family Safety, and Microsoft Outlook Hotmail Connector. Thus,



1 your Affiant seeks more specific authorization to seize and search the OneDrive and  
2 other service data specified in Attachment B of the instant warrant application.

3 **RELEVANT TECHNICAL TERMS**

4 15. The following non-exhaustive list of definitions applies to this Affidavit and  
5 the Attachments to this Affidavit:

6 a. The "Internet" is a worldwide network of computer systems operated  
7 by governmental entities, corporations, and universities. In order to access the Internet,  
8 an individual computer user must subscribe to an access provider, which operates a host  
9 computer system with direct access to the Internet. The World Wide Web is a  
10 functionality of the Internet which allows users of the Internet to share information.

11 b. "Internet Service Providers" are companies that provide access to the  
12 Internet. ISPs can also provide other services for their customers including website  
13 hosting, email service, remote storage, and co-location of computers and other  
14 communications equipment. ISPs offer different ways to access the Internet including  
15 telephone-based (dial-up), broadband-based access via a digital subscriber line (DSL) or  
16 cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge  
17 a fee based upon the type of connection and volume of data (bandwidth). Many ISPs  
18 assign each subscriber an account name, such as a user name, an email address, and an  
19 email mailbox, and the subscriber typically creates a password for his/her account.

20 c. "ISP Records" are records maintained by ISPs pertaining to their  
21 subscribers (regardless of whether those subscribers are individuals or entities). These  
22 records may include account application information, subscriber and billing information,  
23 account access information (often in the form of log files), emails, information concerning  
24

1 content uploaded and/or stored on the ISP's servers, and other information, which may  
2 be stored both in computer data format and in written or printed record format. ISPs  
3 reserve and/or maintain computer disk storage space on their computer system for their  
4 subscribers' use. This service by ISPs allows for both temporary and long-term storage  
5 of electronic communications and many other types of electronic data and files.

6 d. "Online service providers" (also referred to here as "service  
7 providers") are companies that provide online services such as email, chat or instant  
8 messaging, word processing applications, spreadsheet applications, presentation  
9 applications similar to PowerPoint, online calendar, photo storage and remote storage  
10 services. Sometimes they also can provide web hosting, remote storage, and co-location  
11 of computers and other communications equipment. Typically, each service provider  
12 assigns each subscriber an account name, such as a user name or screen name and the  
13 subscriber typically creates a password for his/her account.

14 e. "Computer," as used herein, is defined as "an electronic, magnetic,  
15 optical, electrochemical, or other high speed data processing device performing logical or  
16 storage functions, and includes any data storage facility or communications facility  
17 directly related to or operating in conjunction with such device."

18 f. A "server" is a centralized computer that provides services for other  
19 computers connected to it via a network. The other computers attached to a server are  
20 sometimes called "clients." For example, in a large company, it is common for individual  
21 employees to have client computers at their desktops. When the employees access their  
22 email, or access files stored on the network itself, those files are pulled electronically  
23 from the server, where they are stored, and are sent to the client's computer via the  
24

1 network. Notably, servers can be physically stored in any location: it is not uncommon  
2 for a network's server to be located hundreds (and even thousands) of miles away from  
3 the client computers.

4 g. "Internet Protocol address," or "IP address," refers to a unique  
5 number used by a computer to access the Internet. IP addresses can be dynamic,  
6 meaning that the Internet Service Provider (ISP) assigns a different unique number to  
7 a computer every time it accesses the Internet. IP addresses might also be static, that  
8 is, an ISP assigns a user's computer a particular IP address which is used each time the  
9 computer accesses the Internet.

10 h. The term "domain" refers to a word used as a name for computers,  
11 networks, services, etc. A domain name typically represents a website, a server computer  
12 that hosts that website, or even some computer (or other digital device) connected to the  
13 internet. Essentially, when a website (or a server computer that hosts that website) is  
14 connected to the internet, it is assigned an IP address. Because IP addresses are difficult  
15 for people to remember, domain names are instead used because they are easier to  
16 remember than IP addresses. Domain-names are formed by the rules and procedures of  
17 the Domain Name System (DNS). A common top level domain under these rules is ".com"  
18 for commercial organizations, ".gov" for the United States government, and ".org" for  
19 organizations. For example, [www.usdoj.gov](http://www.usdoj.gov) is the domain name that identifies a server  
20 used by the U.S. Department of Justice, and which uses IP address of 149.101.46.71.

21 i. "Web hosting services" maintain server computers connected to the  
22 Internet. Their customers use those computers to operate websites on the Internet.  
23 Customers of web hosting companies place files, software code, databases, and other data  
24

1 on servers. To do this, customers typically connect from their own computers to the  
2 server computers across the Internet.

3 j. The term “WhoIs” lookup refers to a search of a publicly available  
4 online database that lists information provided when a domain is registered or when an  
5 IP address is assigned.

6 k. The terms “communications,” “records,” “documents,” “programs,” or  
7 “materials” include all information recorded in any form, visual or aural, and by any  
8 means, whether in handmade form (including, but not limited to, writings, drawings,  
9 paintings), photographic form (including, but not limited to, pictures or videos), or  
10 electrical, electronic or magnetic form, as well as digital data files. These terms also  
11 include any applications (i.e. software programs). These terms expressly include, among  
12 other things, emails, instant messages, chat logs, correspondence attached as to emails  
13 (or drafts), calendar entries, buddy lists.

14 l. “Chat” is usually a real time electronic communication between two  
15 or more individuals. Unlike email, which is frequently sent, then read and responded to  
16 minutes, hours, or even days later, chats frequently involve an immediate conversation  
17 between individuals, similar to a face-to-face conversation. Nearly all chat programs are  
18 capable of saving the chat transcript, to enable users to preserve a record of the  
19 conversation. By default, some chat programs have this capability enabled, while others  
20 do not. Many popular web-based email providers, like Microsoft and Microsoft, provide  
21 chat functionality as part of the online services they provide to account holders.

22 ///

23 ///

## FACTS ABOUT EMAIL PROVIDERS

16. In my training, my experience and this investigation, I have learned that Microsoft (the Service Provider) is a company that provides free web-based Internet email access to the general public, and that stored electronic communications, including opened and unopened email for Microsoft subscribers may be located on the computers of Microsoft. I have also learned that Microsoft Inc. provides various on-line service messaging services to the general public. Instant Messaging ("IM") is a form of real-time direct text-based communication between two or more people using shared clients. The text is conveyed via devices connected over a network such as the Internet. In addition to text, Microsoft's software allows users with the most current updated versions to utilize its webcam service. This option enables users from distances all over the world to view others who have installed a webcam on their end. Thus, the Service Provider's servers will contain a wide variety of the subscriber's files, including emails, address books, contact or buddy lists, calendar data, pictures, chat logs, and other files.

17. To use these services, subscribers register for online accounts like the Target Accounts. During the registration process, service providers such as the ones here ask subscribers to provide basic personal information. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit card or bank account number). Based on my training and my experience, I know that subscribers may insert false information to conceal their identity; even if this proves to be the case, however, I know that this information often provide clues to their identity, location or illicit activities.

1           18. In general, when a subscriber receives an email, it is typically stored in the  
2 subscriber's "mail box" on that service provider's servers until the subscriber deletes the  
3 Email. If the subscriber does not delete the message, the message (and any attachments)  
4 can remain on that service provider's servers indefinitely.

5           19. Similarly, when the subscriber sends an email, it is initiated at the  
6 subscriber's computer, transferred via the Internet to the service provider's servers, and  
7 then transmitted to its end destination. That service provider often saves a copy of the  
8 email sent. Unless the sender of the email specifically deletes the Email from the  
9 provider's server, the email can remain on the system indefinitely.

10          20. A sent or received email typically includes the content of the message,  
11 source and destination addresses, the date and time at which the email was sent, and  
12 the size and length of the email. If an email user writes a draft message but does not  
13 send it, that message may also be saved by that service provider, but may not include all  
14 of these categories of data.

15          21. Just as a computer on a desk can be used to store a wide variety of files, so  
16 can online accounts, such as the accounts subject to this application. First, subscribers  
17 can store many types of files as attachments to emails in online accounts. Second,  
18 because service providers provide the services listed above (e.g. word processing,  
19 spreadsheets, pictures), subscribers who use these services usually store documents on  
20 servers maintained and/or owned by service providers. Thus, these online accounts often  
21 contain documents such as pictures, audio or video recordings, logs, spreadsheets,  
22 applications and other files.

22. Reviewing files stored in online accounts raises many of the same difficulties as with reviewing files stored on a local computer. For example, based on my training, my experience and this investigation, I know that subscribers of these online services can conceal their activities by altering files before they upload them to the online service. Subscribers can change file names to more innocuous sounding names (e.g. renaming "FraudRecords.doc" to "ChristmasList.doc"), they can change file extensions to make one kind of file appear like a different type of file (e.g. changing the spreadsheet "StolenCreditProfiles.xls" to "FamilyPhoto.jpg" to appear to be a picture file, where the file extension ".xls" denotes an Excel spreadsheet file and ".jpg" a JPEG format image file), or they can change the times and dates a file was last accessed or modified by changing a computer's system time/date and then uploading that file to the Online Accounts. Thus, to detect any files that the subscriber may have concealed, agents will need to review all of the files in the Target Accounts; they will, however, only seize the items that the Court authorizes to be seized. Similarly, subscribers can conceal their activities by encrypting files. Thus, these files may need to be decrypted to detect whether it constitutes an Item to be Seized.

23. I also believe that people engaged in crimes such as the one described herein often use online accounts because they give people engaged in these crimes a way to easily communicate with other co-conspirators. Moreover, online accounts are easily concealed from law enforcement. Unlike physical documents, electronic documents can be stored in a physical place far away, where they are less likely to be discovered.

24. Service providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the

1 date on which the account was created, the length of service, records of log-in (i.e.,  
2 session) times and durations, the types of service utilized, the status of the account  
3 (including whether the account is inactive or closed), the methods used to connect to the  
4 account (such as logging into the account via websites controlled by the Service  
5 Provider), and other log files that reflect usage of the account. In addition, service  
6 providers often have records of the Internet Protocol address ("IP address") used to  
7 register the account and the IP addresses associated with particular logins to the  
8 account. Because every device that connects to the Internet must use an IP address, IP  
9 address information can help to identify which computers or other devices were used to  
10 access the online account.

11 25. In some cases, subscribers will communicate directly with a service  
12 provider about issues relating to the account, such as technical problems, billing  
13 inquiries, or complaints from or about other users. Service providers typically retain  
14 records about such communications, including records of contacts between the user and  
15 the provider's support services, as well records of any actions taken by the provider or  
16 user as a result of the communications.

17 26. In my training and experience, evidence of who was using an online account  
18 may be found in address books, contact or buddy lists, emails in the account, and pictures  
19 and files, whether stored as attachments or in the suite of the service provider's online  
20 applications. Therefore, the computers of the Service Providers are likely to contain  
21 stored electronic communications (including retrieved and un-retrieved email for their  
22 subscribers) and information concerning subscribers and their use of the provider's  
23  
24



1 services, such as account access information, email transaction information, documents,  
2 pictures, and account application information.

3 27. Microsoft maintains and offers its users the use of OneDrive. OneDrive is  
4 a file-hosting service operated by Microsoft as part of its suite of online services. It allows  
5 users to store files as well as other personal data like Windows settings or BitLocker  
6 recovery keys in the cloud. Files can be synced to a PC and accessed from a web browser  
7 or a mobile device, as well as shared publicly or with specific people. OneDrive offers 5  
8 gigabytes of storage space free of charge; additional storage can be added either  
9 separately or through subscriptions to other Microsoft services including Office 365 and  
10 Groove Music.


11 28. Microsoft offers additional services that may be accessed in relation to and  
12 share associated information with a user's email account, including: Office 365, Windows  
13 Live Mail, Windows Live Writer, Windows Photo Gallery, Windows Live Messenger,  
14 Microsoft Family Safety, and Microsoft Outlook Hotmail Connector.


15 **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

16 29. Your Affiant anticipates executing these warrants under the Electronic  
17 Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and  
18 2703(c)(1)(A), by using the warrant to require Microsoft to disclose to the government  
19 copies of the records and other information (including the content of communications)  
20 particularly described in Section I of Attachment "B." Upon receipt of the information  
21 described in Section I of Attachment "B," government-authorized persons will review  
22 that information to locate the items described in Section II of Attachment "B."

30. Based on the forgoing, I request that the Court issue the proposed search warrant. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

31. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

  
Zachary C. McKinney, Special Agent  
Federal Bureau of Investigation

  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT "A-1"**

**ONLINE ACCOUNT TO BE SEARCHED**

This warrant applies to information associated with the Microsoft email account centralpark1@live.com (the "Target Account 1") from inception to present, which is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, headquartered at 1 Microsoft Way, Redmond, Washington, 98052.

**ATTACHMENT "A-2"**

**ONLINE ACCOUNT TO BE SEARCHED**

This warrant applies to information associated with the Microsoft email account marilouroses@live.com (the "Target Account 2") from inception to present, which is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, headquartered at 1 Microsoft Way, Redmond, Washington, 98052.

**ATTACHMENT "B"**  
**Particular Things to be Seized**

**I. Information to be disclosed by the Service Provider**

To the extent that the information described in Attachments A1 and A2 is within the possession, custody, or control of Microsoft, including any Emails, records, files, logs, or information that have been deleted but are still available to Service Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Service Provider is required to disclose the following information to the government for each account or identifier listed in Attachments A-1 and A-2 from account inception to present:

- a. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any OneDrive accounts associated with or assigned to Target Accounts 1 and 2.
- b. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Office 360 accounts associated with or assigned to Target Accounts 1 and 2.
- c. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Microsoft Family Safety accounts or services associated with or assigned to Target Accounts 1 and 2.
- d. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Windows Live Writer accounts or services associated with or assigned to Target Accounts 1 and 2.
- e. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Windows Live Mail accounts or services associated with or assigned to Target Accounts 1 and 2.
- f. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Windows Photo Gallery accounts or services associated with or assigned to Target Accounts 1 and 2.
- g. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Windows Live Messenger accounts or services associated with or assigned to Target Accounts 1 and 2.

1           **II.     Information to be seized by the United States**

2           After reviewing all information described in Section I, the United States will seize  
3 evidence of violations of Title 18, United States Code Sections 32(a)  
4 (Destruction/Damage of Aircraft or Aircraft Facilities); 37(a)(2) (Violence at  
5 International Airport); and 922(a)(3); and 5 (Unlawful Interstate Transport/Delivery of  
Firearms by Non Federal Firearms Licensee); and 2 (Aiding and Abetting) (the "Subject  
Offenses") that occur in the form of the following, from account inception to present:

- 6           a.     Communications, transactions and records that may establish ownership  
7 and control (or the degree thereof) of the Target Account, including address  
8 books, contact or buddy lists, bills, invoices, receipts, registration records,  
9 bills, correspondence, notes, records, memoranda, telephone/address books,  
10 photographs, video recordings, audio recordings, lists of names, records of  
11 payment for access to newsgroups or other online subscription services, and  
12 attachments to said communications, transactions and records.
- 13           b.     Communications, transactions and records to/from persons who may be co-  
14 conspirators of the Subject Offenses, or which may identify co-conspirators.
- 15           c.     Communications, transactions and records which may show motivation to  
16 commit the Subject Offenses.
- 17           d.     Communications, transactions and records that relate to the Subject  
18 Offenses.
- 19           e.     The terms "communications," "transactions," "records," "documents,"  
20 "programs," or "materials" include all information recorded in any form,  
21 visual or aural, and by any means, whether in handmade form (including,  
22 but not limited to, writings, drawings, paintings), photographic form  
23 (including, but not limited to, pictures or videos), or electrical, electronic or  
24 magnetic form, as well as digital data files. These terms also include any  
applications (i.e. software programs). These terms expressly include, among  
other things, Emails, instant messages, chat logs, correspondence attached  
as to Emails (or drafts), calendar entries, buddy lists.

**ATTACHMENT "C"****PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED  
PURSUANT TO THIS SEARCH WARRANT**

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B, Section II. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B, Section II. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B, Section II as Information to be Seized, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

5. The search procedures utilized for this review are at the sole discretion of the investigating and prosecuting authorities, and may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in the Search Warrant Data to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover from the Search Warrant Data any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

- c. surveying various file directories and the individual files they contain;

- d. opening files in order to determine their contents;

- e. using hash values to narrow the scope of what may be found. Hash values are under-inclusive, but are still a helpful tool;

f. scanning storage areas;

g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A1 and A2; and/or

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B, Section II.

## Return and Review Procedures

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:



1 (i) execute the warrant within a specified time no longer than 14 days;

2 (B) Warrant Seeking Electronically Stored Information. A warrant under Rule  
3 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or  
4 copying of electronically stored information. Unless otherwise specified, the warrant  
5 authorizes a later review of the media or information consistent with the warrant. The  
6 time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or  
7 on-site copying of the media or information, and not to any later off-site copying or  
8 review.

6 (f) Executing and Returning the Warrant.

7 (1) Warrant to Search for and Seize a Person or Property.

8 (B) Inventory. An officer present during the execution of the warrant must prepare  
9 and verify an inventory of any property seized. . . . In a case involving the seizure of  
10 electronic storage media or the seizure or copying of electronically stored information,  
11 the inventory may be limited to describing the physical storage media that were seized  
12 or copied. The officer may retain a copy of the electronically stored information that was  
13 seized or copied.

12 7. Pursuant to this Rule, the government understands and will act in  
13 accordance with the following:

14 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution  
15 of the warrant, an agent is required to file an inventory return with the Court, that is,  
16 to file an itemized list of the property seized. Execution of the warrant begins when  
17 the United States serves the warrant on the named custodian; execution is complete  
18 when the custodian provides all Search Warrant Data to the United States. Within  
19 fourteen (14) days of completion of the execution of the warrant, the inventory will be  
20 filed.

18 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within  
19 which the electronically stored information must be seized after the issuance of the  
20 warrant and copied after the execution of the warrant, not the "later review of the media  
21 or information" seized, or the later off-site digital copying of that media.

22 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court  
23 may be limited to a description of the "physical storage media" into which the Search  
24 Warrant Data that was seized was placed, not an itemization of the information or data  
25 stored on the "physical storage media" into which the Search Warrant Data was placed;

1 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for  
2 purposes of the investigation. The government proposes that the original storage media  
3 on which the Search Warrant Data was placed plus a full image copy of the seized Search  
Warrant Data be retained by the government.

4 e. If the person from whom any Search Warrant Data was seized requests the return  
5 of any information in the Search Warrant Data that is not set forth in Attachment B,  
6 Section II, that information will be copied onto appropriate media and returned to the  
7 person from whom the information was seized.  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24



FILED

2017 OCT 13 PM 12:36

U.S. MAGISTRATE JUDGE

BY \_\_\_\_\_

SEALED

Office of the United States Attorney  
District of Nevada  
501 Las Vegas Boulevard, Suite 1100  
Las Vegas, Nevada 89101  
(702) 388-6336

**FILED**

2017 OCT 13 PM 12:36

U.S. MAGISTRATE JUDGE

BY \_\_\_\_\_

STEVEN W. MYHRE  
Acting United States Attorney  
District of Nevada  
CRISTINA D. SILVA  
PATRICK BURNS  
Assistant United States Attorneys  
501 Las Vegas Blvd. South, Ste. 1100  
Las Vegas, Nevada 89101  
Telephone: (702) 388-6336  
Fax (702) 388-6698  
[john.p.burns@usdoj.gov](mailto:john.p.burns@usdoj.gov)

Attorney for the United States of America

**UNITED STATES DISTRICT COURT  
DISTRICT OF NEVADA**

-oOo-

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH:  
EMAIL ACCOUNT  
CENTRALPARK1@LIVE.COM THAT IS  
STORED AT A PREMISES CONTROLLED  
BY MICROSOFT. A1

**Magistrate No.**

**(Under Seal)**

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH:  
EMAIL ACCOUNT  
MARILOUROSES@LIVE.COM THAT IS  
STORED AT A PREMISES CONTROLLED  
BY MICROSOFT A2

**Magistrate No. 2:17-mj-01010-NJK**

**(Under Seal)**

**GOVERNMENT'S APPLICATION REQUESTING  
SEALING OF AFFIDAVIT**

COMES NOW the United States of America, by and through STEVEN W.  
MYHRE, Acting United States Attorney, and PATRICK BURNS, Assistant United States  
Attorney, and respectfully moves this Honorable Court for an Order sealing the Affidavit,

1 together with the Court's Order, in the above-captioned matter until such time as this Honorable  
2 Court, or another Court of competent jurisdiction, shall order otherwise.

3 The Government submits that it is necessary for said documents to be sealed in light of  
4 the fact that they make reference to information regarding an on-going investigation. The  
5 Government submits that disclosure of the information might possibly jeopardize the  
6 investigation. The Government submits that its right to secrecy far outweighs the public's right  
7 to know.  
8

9 DATED this 12 day of October 2017.

10  
11 Respectfully submitted,  
12 STEVEN W. MYHRE  
13 Acting United States Attorney

14 

15 PATRICK BURNS  
16 Assistant United States Attorney  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26

FILED

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

2017 OCT 13 PM 12:36

U.S. MAGISTRATE JUDGE

BY \_\_\_\_\_

-oOo-

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH:  
EMAIL ACCOUNT  
CENTRALPARK1@LIVE.COM THAT IS  
STORED AT A PREMISES CONTROLLED  
BY MICROSOFT. A1

Magistrate No.

(Under Seal)

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH:  
EMAIL ACCOUNT  
MARILOUROSES@LIVE.COM THAT IS  
STORED AT A PREMISES CONTROLLED  
BY MICROSOFT A2

Magistrate No. 2:17-mj-01010-NJK

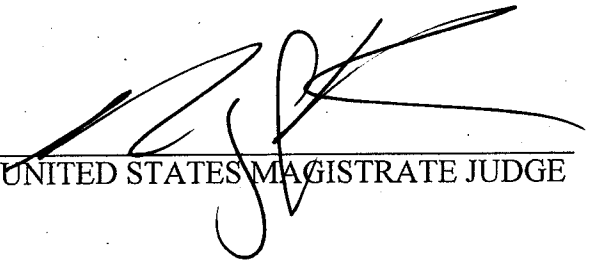
(Under Seal)

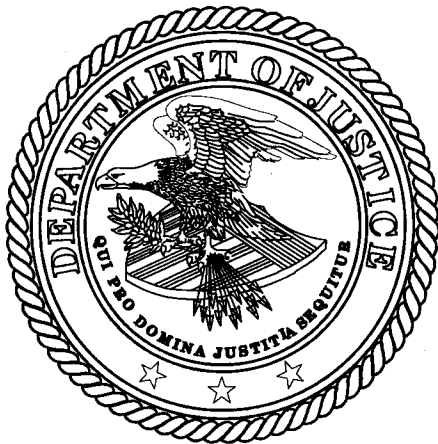
SEALING ORDER

Based on the pending Application of the Government, and good cause appearing therefor,

IT IS HEREBY ORDERED that the Affidavit, together with the Court's Order, in  
the above-captioned matter shall be sealed until further Order of the Court.

DATED this 13<sup>th</sup> day of October, 2017.

  
UNITED STATES MAGISTRATE JUDGE



FILED

2017 OCT 13 PM 12:36

U.S. MAGISTRATE JUDGE

BY \_\_\_\_\_

SEALED

Office of the United States Attorney  
District of Nevada  
501 Las Vegas Boulevard, Suite 1100  
Las Vegas, Nevada 89101  
(702) 388-6336

**FILED****UNITED STATES DISTRICT COURT  
DISTRICT OF NEVADA****2017 OCT 13 PM 12: 36****-oOo-****U.S. MAGISTRATE JUDGE****BY \_\_\_\_\_**

IN THE MATTER OF THE SEARCH ) Mag. Case No: 2:17-mj-  
 OF INFORMATION ASSOCIATED ) ORDER COMMANDING  
 WITH EMAIL ACCOUNT ) MICROSOFT CORPORATION NOT  
 CENTRALPARK1@LIVE.COM THAT ) TO NOTIFY ANY PERSON OF THE  
 IS STORED AT PREMISES ) EXISTENCE OF SEARCH WARRANT  
 CONTROLLED BY MICROSOFT. A1 ) **Under Seal**

IN THE MATTER OF THE SEARCH ) Mag. Case No: 2:17-mj-01010-NJK  
 OF INFORMATION ASSOCIATED ) ORDER COMMANDING  
 WITH EMAIL ACCOUNT ) MICROSOFT CORPORATION NOT  
 MARILOUROSES@LIVE.COM THAT ) TO NOTIFY ANY PERSON OF THE  
 IS STORED AT PREMISES ) EXISTENCE OF SEARCH WARRANT  
 CONTROLLED BY MICROSOFT. A2 ) **Under Seal**

The United States has submitted an application pursuant to 18 U.S.C. § 2705(b), requesting that the Court issue an Order commanding Microsoft Corporation, located at 1355 Market Street, Suite 900, San Francisco, California 94103, an electronic communication service provider and/or a remote computing service, not to notify any person (including the subscribers and customers of the account(s) listed in the search warrant) of the existence of the attached search warrant until further order of the Court.

The Court determines that there is reason to believe that notification of the existence of the attached search warrant will seriously jeopardize the investigation or unduly delay a trial, including the following: giving the targets an opportunity to change patterns of behavior, change online personas, change or modify email addresses or other online user IDs, flee or continue flight from prosecution, destroy or tamper with evidence, intimidate potential witnesses, engage in additional extortion, or cause the release of the images that are the subject of the investigation



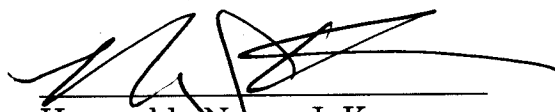
1 causing substantial personal and reputational harm to the victim. See 18 U.S.C. §  
2 2705(b).

3 IT IS THEREFORE ORDERED under 18 U.S.C. § 2705(b) that Microsoft  
4 Corporation shall not disclose the existence of the attached search warrant, or this  
5 Order of the Court, to the listed subscriber or to any other person, unless and until  
6 otherwise authorized to do so by the Court, except that Microsoft Corporation may  
7 disclose the attached search warrant to an attorney for Microsoft Corporation for the  
purpose of receiving legal advice.

8 IT IS FURTHER ORDERED that the application and this Order are sealed  
until otherwise ordered by the Court.

9  
10 Oct. 13, 2017

11 Date

  
Honorable Nancy J. Koppe  
United States Magistrate Judge

FILED

2017 OCT 13 PM 12:36

U.S. MAGISTRATE JUDGE

BY \_\_\_\_\_



SEALED

Office of the United States Attorney  
District of Nevada  
501 Las Vegas Boulevard, Suite 1100  
Las Vegas, Nevada 89101  
(702) 388-6336

**FILED**

**UNITED STATES DISTRICT COURT  
DISTRICT OF NEVADA**

2017 OCT 13 PM 12:36

-oOo-

U.S. MAGISTRATE JUDGE

IN THE MATTER OF THE SEARCH )  
 OF INFORMATION ASSOCIATED )  
 WITH EMAIL ACCOUNT )  
 CENTRALPARK1@LIVE.COM THAT )  
 IS STORED AT PREMISES )  
 CONTROLLED BY MICROSOFT. A1 )

Mag. Case No: 2:17-mj-  
 ORDER COMMANDING  
 MICROSOFT CORPORATION NOT  
 TO NOTIFY ANY PERSON OF THE  
 EXISTENCE OF SEARCH WARRANT  
**Under Seal**

IN THE MATTER OF THE SEARCH )  
 OF INFORMATION ASSOCIATED )  
 WITH EMAIL ACCOUNT )  
 MARILOUROSES@LIVE.COM THAT )  
 IS STORED AT PREMISES )  
 CONTROLLED BY MICROSOFT. A2 )

Mag. Case No: 2:17-mj-01010-NJK  
 ORDER COMMANDING  
 MICROSOFT CORPORATION NOT  
 TO NOTIFY ANY PERSON OF THE  
 EXISTENCE OF SEARCH WARRANT  
**Under Seal**

The United States has submitted an application pursuant to 18 U.S.C. § 2705(b), requesting that the Court issue an Order commanding Microsoft Corporation, located at 1355 Market Street, Suite 900, San Francisco, California 94103, an electronic communication service provider and/or a remote computing service, not to notify any person (including the subscribers and customers of the account(s) listed in the search warrant) of the existence of the attached search warrant until further order of the Court.

The Court determines that there is reason to believe that notification of the existence of the attached search warrant will seriously jeopardize the investigation or unduly delay a trial, including the following: giving the targets an opportunity to change patterns of behavior, change online personas, change or modify email addresses or other online user IDs, flee or continue flight from prosecution, destroy or tamper with evidence, intimidate potential witnesses, engage in additional extortion, or cause the release of the images that are the subject of the investigation

1 causing substantial personal and reputational harm to the victim. See 18 U.S.C. §  
2 2705(b).

3 IT IS THEREFORE ORDERED under 18 U.S.C. § 2705(b) that Microsoft  
4 Corporation shall not disclose the existence of the attached search warrant, or this  
5 Order of the Court, to the listed subscriber or to any other person, unless and until  
6 otherwise authorized to do so by the Court, except that Microsoft Corporation may  
7 disclose the attached search warrant to an attorney for Microsoft Corporation for the  
8 purpose of receiving legal advice.

9 IT IS FURTHER ORDERED that the application and this Order are sealed  
10 until otherwise ordered by the Court.

11 10/13/17  
12 Date

13 NANCY J. KOPPE  
14 \_\_\_\_\_  
15 Honorable Nancy J. Koppe  
16 United States Magistrate Judge

17 I hereby attest and certify on 10/13/17  
18 that the foregoing document is a full true and correct  
19 copy of the original on file in my office, and in my legal  
20 custody.

21 NANCY J. KOPPE  
22 U.S. MAGISTRATE JUDGE  
23 DISTRICT OF NEVADA

By [Signature] Deputy  
Clerk

FILED

## UNITED STATES DISTRICT COURT

2017 OCT 13 PM 12:36

for the  
District of Nevada

U.S. MAGISTRATE JUDGE

BY \_\_\_\_\_

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

Case No. 2:17-mj-01010-NJK

EMAIL ACCOUNT MARILOUROSES@LIVE.COM THAT  
IS STORED AT A PREMISES CONTROLLED BY  
MICROSOFT. A2

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search  
of the following person or property located in the \_\_\_\_\_ District of \_\_\_\_\_ Nevada  
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A2

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property  
described above, and that such search will reveal (identify the person or describe the property to be seized):

SEE ATTACHMENTS B and C

**YOU ARE COMMANDED** to execute this warrant on or before October 27, 2017 (not to exceed 14 days)☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the  
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the  
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory  
as required by law and promptly return this warrant and inventory to Rory J. Koppe  
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.  
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose  
property, will be searched or seized (check the appropriate box)☐ for \_\_\_\_\_ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of \_\_\_\_\_

Date and time issued:

10/13/2017 12:30 pm

City and state:

Las Vegas, Nevada

Judge's signature

Printed name and title

Rory J. Koppe, US Magistrate Judge

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

**Return**

Case No.:

2:17-mj-

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Executing officer's signature*\_\_\_\_\_  
*Printed name and title*



SEALED

**Office of the United States Attorney**  
District of Nevada  
501 Las Vegas Boulevard, Suite 1100  
Las Vegas, Nevada 89101  
(702) 388-6336

ATTACHMENT "A-2"

ONLINE ACCOUNT TO BE SEARCHED

This warrant applies to information associated with the Microsoft email account marilouroses@live.com (the "Target Account 2") from inception to present, which is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, headquartered at 1 Microsoft Way, Redmond, Washington, 98052.



**ATTACHMENT "B"**  
**Particular Things to be Seized**

**I. Information to be disclosed by the Service Provider**

To the extent that the information described in Attachments A1 and A2 is within the possession, custody, or control of Microsoft, including any Emails, records, files, logs, or information that have been deleted but are still available to Service Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Service Provider is required to disclose the following information to the government for each account or identifier listed in Attachments A-1 and A-2 from account inception to present:

- a. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any OneDrive accounts associated with or assigned to Target Accounts 1 and 2.
- b. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Office 360 accounts associated with or assigned to Target Accounts 1 and 2.
- c. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Microsoft Family Safety accounts or services associated with or assigned to Target Accounts 1 and 2.
- d. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Windows Live Writer accounts or services associated with or assigned to Target Accounts 1 and 2.
- e. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Windows Live Mail accounts or services associated with or assigned to Target Accounts 1 and 2.
- f. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Windows Photo Gallery accounts or services associated with or assigned to Target Accounts 1 and 2.
- g. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Windows Live Messenger accounts or services associated with or assigned to Target Accounts 1 and 2.

1       II.     **Information to be seized by the United States**

2       After reviewing all information described in Section I, the United States will seize  
3 evidence of violations of Title 18, United States Code Sections 32(a)  
4 (Destruction/Damage of Aircraft or Aircraft Facilities); 37(a)(2) (Violence at  
5 International Airport); and 922(a)(3); and 5 (Unlawful Interstate Transport/Delivery of  
Firearms by Non Federal Firearms Licensee); and 2 (Aiding and Abetting) (the "Subject  
Offenses") that occur in the form of the following, from account inception to present:

- 6       a.     Communications, transactions and records that may establish ownership  
7 and control (or the degree thereof) of the Target Account, including address  
8 books, contact or buddy lists, bills, invoices, receipts, registration records,  
9 bills, correspondence, notes, records, memoranda, telephone/address books,  
10 photographs, video recordings, audio recordings, lists of names, records of  
11 payment for access to newsgroups or other online subscription services, and  
12 attachments to said communications, transactions and records.
- 13       b.     Communications, transactions and records to/from persons who may be co-  
14 conspirators of the Subject Offenses, or which may identify co-conspirators.
- 15       c.     Communications, transactions and records which may show motivation to  
16 commit the Subject Offenses.
- 17       d.     Communications, transactions and records that relate to the Subject  
18 Offenses.
- 19       e.     The terms "communications," "transactions," "records," "documents,"  
20 "programs," or "materials" include all information recorded in any form,  
21 visual or aural, and by any means, whether in handmade form (including,  
22 but not limited to, writings, drawings, paintings), photographic form  
23 (including, but not limited to, pictures or videos), or electrical, electronic or  
24 magnetic form, as well as digital data files. These terms also include any  
applications (i.e. software programs). These terms expressly include, among  
other things, Emails, instant messages, chat logs, correspondence attached  
as to Emails (or drafts), calendar entries, buddy lists.

**ATTACHMENT "C"****PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED  
PURSUANT TO THIS SEARCH WARRANT**

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B, Section II. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B, Section II. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B, Section II as Information to be Seized, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

5. The search procedures utilized for this review are at the sole discretion of the investigating and prosecuting authorities, and may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in the Search Warrant Data to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover from the Search Warrant Data any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

- e. using hash values to narrow the scope of what may be found. Hash values are under-inclusive, but are still a helpful tool;

f. scanning storage areas;

g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A1 and A2; and/or

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B, Section II.

## Return and Review Procedures

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

1 (i) execute the warrant within a specified time no longer than 14 days;

2 (B) Warrant Seeking Electronically Stored Information. A warrant under Rule  
3 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or  
4 copying of electronically stored information. Unless otherwise specified, the warrant  
5 authorizes a later review of the media or information consistent with the warrant. The  
6 time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or  
7 on-site copying of the media or information, and not to any later off-site copying or  
8 review.

6 (f) Executing and Returning the Warrant.

7 (1) Warrant to Search for and Seize a Person or Property.

8 (B) Inventory. An officer present during the execution of the warrant must prepare  
9 and verify an inventory of any property seized. . . . In a case involving the seizure of  
10 electronic storage media or the seizure or copying of electronically stored information,  
11 the inventory may be limited to describing the physical storage media that were seized  
12 or copied. The officer may retain a copy of the electronically stored information that was  
13 seized or copied.

12 7. Pursuant to this Rule, the government understands and will act in  
13 accordance with the following:

14 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution  
15 of the warrant, an agent is required to file an inventory return with the Court, that is,  
16 to file an itemized list of the property seized. Execution of the warrant begins when  
17 the United States serves the warrant on the named custodian; execution is complete  
18 when the custodian provides all Search Warrant Data to the United States. Within  
19 fourteen (14) days of completion of the execution of the warrant, the inventory will be  
20 filed.

21 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within  
22 which the electronically stored information must be seized after the issuance of the  
23 warrant and copied after the execution of the warrant, not the "later review of the media  
24 or information" seized, or the later off-site digital copying of that media.

25 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court  
26 may be limited to a description of the "physical storage media" into which the Search  
27 Warrant Data that was seized was placed, not an itemization of the information or data  
28 stored on the "physical storage media" into which the Search Warrant Data was placed;

1 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for  
2 purposes of the investigation. The government proposes that the original storage media  
3 on which the Search Warrant Data was placed plus a full image copy of the seized Search  
Warrant Data be retained by the government.

4 e. If the person from whom any Search Warrant Data was seized requests the return  
5 of any information in the Search Warrant Data that is not set forth in Attachment B,  
6 Section II, that information will be copied onto appropriate media and returned to the  
7 person from whom the information was seized.  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

| Return   |  |   |
|--|--|---|
| Case No.:<br>2:17-mj- 01010-NJK  | Date and time warrant executed:<br>10/15/2017, 07:40AM | Copy of warrant and inventory left with:<br>MICROSOFT VIA FAX TO (425) 708-0096 |
| Inventory made in the presence of:   |  |   |
| <p>Inventory of the property taken and name of any person(s) seized:</p> <p style="margin-left: 40px;">THIS WARRANT WAS A SUPPLEMENTAL WARRANT FOR THE CONTENTS OF A ONEDRIVE ACCOUNT AFTER THE SEARCH WARRANT IN 2:17-mj-967-NJK. THE ONE DRIVE ACCOUNT WAS PRODUCED AND REVIEWED ON 01/31/2018 AND WAS FOUND TO HAVE NO CONTENTS. OTHER ITEMS PRODUCED HAD PREVIOUSLY BEEN PRODUCED.</p> <div style="text-align: right; margin-top: 100px;"> <p><b>FILED</b></p> <p>2018 FEB -2 PM 1:25</p> <p>U.S. MAGISTRATE JUDGE</p> <p>BY _____</p> </div>            |  |   |
| Certification  |  |   |
| <p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between; margin-top: 20px;"> <div style="width: 30%;"> <p>Date: <u>02/02/2018</u></p> </div> <div style="width: 60%; text-align: center;"> <p><u>T. Todd Tumbleson</u></p> <p><small>Executing officer's signature</small></p> <p><u>T. TODD TUMBLESON</u></p> <p><u>SA, FBI, LV, NV</u></p> <p><small>Printed name and title</small></p> </div> </div> |  |   |